Another Lattice Attack Against an RSA-like Cryptosystem

George Teşeleanu[1,2]

[1] Advanced Technologies Institute
10 Dinu Vintilă, Bucharest, Romania
tgeorge@dcti.ro
[2] Simion Stoilow Institute of Mathematics of the Romanian Academy
21 Calea Grivitei, Bucharest, Romania

Abstract. Let $N = pq$ be the product of two balanced prime numbers p and q. In 2015, Roman'kov introduced an interesting RSA-like cryptosystem that, unlike the classical RSA key equation $ed - k(p-1)(q-1) = 1$, uses the key equation $ed - kr = 1$, where $r|p-1$ and is a large prime number. In this paper, we study if small private key attacks based on lattices can be applied to Roman'kov's cryptosystem. More precisely, we argue that such attacks do not appear to be applicable to this scheme without substantial adaptations.

Keywords: lattice attack, small private key attack, RSA

1 Introduction

RSA is one of the most widely adopted cryptosystems and was designed by Rivest, Shamir and Adleman [16] in 1978. The standard version of RSA has as an underlying group $\mathbb{Z}_N^*$, where N is the product of two large prime numbers p and q. To encrypt a message m such that $m < N$, the process involves computing $c \equiv m^e \bmod N$, where e satisfies $\gcd(e, \varphi(N)) = 1$ and $\varphi(N) = (p-1)(q-1)$ is Euler's totient function. The inverse operation requires computing $m \equiv c^d \bmod N$, where $d \equiv e^{-1} \bmod \varphi(N)$. Note that (N, e) are public, while (p, q, d) are kept secret. The standard RSA, termed balanced RSA, employs primes p and q that have the same bit-size (*i.e.* $q < p < 2q$). This paper exclusively focuses on balanced RSA and its variations.

In parallel with the development of modulus factoring methods, several specific attacks have been developed in order to extract as much information as possible from the public key (N, e). Therefore, Wiener showed in [19] that if $d < N^{0.25}/3$, then one can retrieve d from the continued fraction expansion of e/N, and thus factor N. This bound was improved by Boneh and Durfee [3] to $N^{0.292}$. The main tools that they used are Coppersmith's method [5] and lattice reduction techniques [12]. Later on, Herrmann and May [8] obtain the same bound, but using simpler techniques. For more details about RSA attacks we refer the reader to [2, 14, 18].

A variant of RSA was proposed by Roman'kov [17] in 2015. Compared to the classical RSA, this new proposal is randomized, and factoring N does not lead to recovering encrypted messages. To achieve these properties, Roman'kov considers two distinct subgroups of $\mathbb{M}, \mathbb{H} \subset \mathbb{Z}_n$, one of order r and the other of order t, where r and t are prime numbers. In this scheme, the encryption exponent is chosen such that $\gcd(e, r) = 1$, and the corresponding decryption exponent is computed as $d = td_1$, where $d_1 \equiv (te)^{-1} \bmod r$. The encryption and decryption processes are similar to RSA. More precisely, to encrypt a message $m \in \mathbb{M}$, we compute $c \equiv (hm)^e \bmod N$, where h is a random element from $\mathbb{H}$. To decrypt, we simply compute $m \equiv c^d \bmod N$.

In this paper, we provide the first security analysis of Roman'kov's scheme. We argue that lattice based attacks do not seem to work against this cryptosystem. To substantiate our claims, we show that the results provided in [1, 11] cannot be applied. Given that the result presented in [11] is optimal under certain reasonable assumptions, we conclude that this class of attacks do not seem to work against the Roman'kov cryptosystem without substantial adaptations.

Structure of the Paper. Preliminary notions are provided in Section 2. In Section 3 we describe our impossibility results. We conclude our paper in Section 4.

2 Preliminaries

Notations. Throughout the paper, λ and τ denote security parameters. Also, the notation $|S|$ denotes the cardinality of a set S. By $|n|$ we denote the size of n in bits. We use $\simeq$ to indicate that two values are approximately equal. The action of selecting a random element x from a sample space X is denoted by $x \xleftarrow{\$} X$.

2.1 RSA-like Cryptosystem

Instead of choosing the message space as the entire $\mathbb{Z}_N^*$ group, Roman'kov [17] selects two subgroups $\mathbb{M}, \mathbb{H} \subset \mathbb{Z}_N^*$ and encrypts only messages from $\mathbb{M}$. This approach allows the sender to use random elements from $\mathbb{H}$ to mask the message. We further present the cryptosystem as described in [17].

Setup(λ, τ): Randomly generate two distinct large prime numbers r and t such that $|r| = |t| = \lambda$. Choose randomly two integers α and β such that $|\alpha| = |\beta| = \tau$ until $p = 2\alpha r + 1$ and $q = 2\beta t + 1$ are both prime. Compute the product $N = pq$. Choose generators u and v such that their order are r and t, respectively. Choose an integer e such that $\gcd(e, r) = 1$ and compute d_1 such that $ted_1 \equiv 1 \bmod r$. Output the public key $pk = (N, e, u, v, \mathbb{M}, \mathbb{H})$, where $\mathbb{M} = \langle u \rangle$ and $\mathbb{H} = \langle v \rangle$. The corresponding secret key is $sk = (p, q, r, t, d)$, where $d = td_1$.

Encrypt(pk, m): To encrypt a message $m \in \mathbb{M}$ we choose a random element $h \xleftarrow{\$} \mathbb{H}$ and then we compute $c \equiv (hm)^e \bmod N$. Output the ciphertext c.

Decrypt(sk, c): To recover the message, simply compute $m \equiv c^d \bmod N$.

Remark 1. When choosing the public key, we have to select two generators. An effective way to accomplish this is to first randomly choose the value $u_1 \xleftarrow{\$} \mathbb{Z}_p^*$ until the order of u_1 is r. Using the Chinese Remainder Theorem, we compute the desired value $u \in \mathbb{Z}_n^*$ such that $u \equiv u_1 \bmod p$ and $u \equiv 1 \bmod q$. A similar process applies for v.

2.2 Useful Lemmas

The results provided in this section will be used in Section 3 to bound the solutions of equations $xy+1 \equiv 0 \bmod e$ and $xH(y) - 4\alpha\beta t \equiv 0 \bmod e$, which are derived from the key equation[3] $ed - kr = 1$. We start by providing lower and upper bounds for p and q (see [15, Lemma 1]).

Lemma 1. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following property holds*

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}.$$

The bounds for $\varphi(N)$ are provided in [7, Corollary 1]. This result implies that $\varphi(N)$ can be approximated by N.

Corollary 1. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following property holds*

$$\left(\sqrt{N} - 1\right)^2 > \varphi(N) > N\left(1 - \frac{3}{\sqrt{2N}}\right) + 1.$$

2.3 Finding Small Roots

In this section, we outline some tools used for solving the problem of finding small roots, both in the modular and integer cases.

Coppersmith [4–6] provided rigorous techniques for computing small integer roots of single-variable polynomials modulo an integer, as well as bivariate polynomials over the integers. In the case of modular roots, Coppersmith's ideas were reinterpreted by Howgrave-Graham [9]. We further provide Howgrave-Graham result.

Theorem 1. *Let $f(x_1, \ldots, x_n) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial with at most ω monomials, α be an integer and let*

$$||f(x_1, \ldots, x_n)|| = \sqrt{\sum |a_{i_1 \ldots i_n}|^2}$$

be its norm. Suppose that

- *$f(y_1, \ldots, y_n) \equiv 0 \bmod \alpha$ for some $|y_1| < X_1, \ldots, |y_n| < X_n$,*

[3] equivalently written as $ed - k\varphi(N)/4\alpha\beta t = 1$, since $r = \varphi(N)/4\alpha\beta t$

– $||f(y_1X_1, \ldots, y_nX_n)|| < \alpha/\sqrt{\omega}$,

then $f(y_1, \ldots, y_n) = 0$ *holds over integers.*

Lenstra, Lenstra and Lovász [12] proposed a lattice reduction algorithm (LLL) that is widely used in cryptanalysis and is typically combined with Howgrave-Graham's lemma. We further provide the version presented in [10,13].

Theorem 2. *Let L be a lattice of dimension ω. In polynomial time, the LLL algorithm outputs a reduced basis $(b_1, \ldots, b_\omega)$ that satisfies*

$$||b_1|| \leq \ldots \leq ||b_i|| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} det(L)^{\frac{1}{\omega+1-i}},$$

where $det(L)$ is the determinant of lattice L.

Note that the condition

$$2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} det(L)^{\frac{1}{\omega+1-i}} < \alpha/\sqrt{\omega}$$

implies that the polynomials corresponding to b_i match Howgrave-Graham's bound. This leads to

$$det(L) \leq \varepsilon \alpha^{\omega+1-i},$$

where ε is an error term that is usually ignored.

In order to find a solution $(y_1, \ldots, y_n)$ we need the following assumption to be true.

Assumption 3 *The LLL reduced basis polynomials are algebraically independent*[4]*, and the resultant computations for b_i yields the common roots of these polynomials.*

In [11], a lattice based method for finding small solutions of the equation $xH(y) + c \equiv 0 \bmod \beta$ is provided. This result extensions the Boneh and Durfee method [3] and uses the LLL algorithm [12] and Howgrave-Graham's lemma [9] to derive the solutions. The author shows that the bounds provided in [11] are optimal under reasonable assumptions. Note that, using a different lattice construction the authors of [1] prove a similar result.

Theorem 4. *Let $H(y) \in \mathbb{Z}[y]$ be a monic polynomial with degree $r \geq 1$ and β be an integer. Suppose that*

– $x_0H(y_0) + c \equiv 0 \bmod \beta$ *for some* $|x_0| < X = \beta^\delta, |y_0| < Y = \beta^\gamma$,
– $|c| < XY^r$,

then one can solve the equation $xH(y) + c \equiv 0 \bmod \beta$ if

$$\begin{cases} \delta \leq \frac{r+2}{2(r+1)} - \frac{r+1}{2}\gamma & \text{when } 0 < \gamma < r/(r+1)^2, \\ \delta \leq 1 - \sqrt{r\gamma}, & \text{when } r/(r+1)^2 \leq \gamma \leq 1/r. \end{cases}$$

[4] they do not share a non-trivial gcd

3 Application of Lattices

We further provide two negative results. Namely, that we cannot devise a lattice based attack to factor N or recover r in polynomial time using the results presented in [1, 11].

Theorem 5. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $e = N^{\delta}$, $2^{\tau+2} = N^{\varepsilon}$ and $d < N^{\gamma}$. We cannot factor N in polynomial time using the method presented in Theorem 4.*

Proof. Note that

$$\varphi(N) = N - (p+q) + 1$$

and thus, finding $p+q$ is equivalent to solving the equation

$$h(y) = -y + N + 1,$$

or analogously the monic polynomial $H(y) = -h(y)$.

By rewriting the key equation $ed - k\varphi(N)/4\alpha\beta t = 1$, we obtain the congruence $k\varphi(N) + 4\alpha\beta t \equiv 0 \bmod e$, that is equivalent to $k(-\varphi_n(N)) - 4\alpha\beta t \equiv 0 \bmod e$. Consequently, we deduce the equation $xH(y) - 4\alpha\beta t \equiv 0 \bmod e$, which has k and $p+q$ as solutions.

In order to be able to apply Theorem 4 we first need to bound k and $p+q$. Since we have

- $k\varphi(N) = 4\alpha\beta t(ed-1) < 4\alpha\beta ted$,
- $\alpha < 2^{\tau+1} = N^{\varepsilon}/2$,
- $2\beta t = q - 1 < \sqrt{N}$ (see Lemma 1),
- $N \simeq \varphi(N)$ (see Corollary 1),

we obtain that

$$k < \frac{4\alpha\beta ted}{\varphi(N)} < N^{\delta+\gamma+\varepsilon-0.5}.$$

Using Lemma 1 we have that $p+q < 3\sqrt{N}$. Therefore, we have that $k < X = e^{(\delta+\gamma+\varepsilon-0.5)/\delta}$ and $p+q < Y \simeq e^{0.5/\delta}$.

Note that, we also need

$$|-4\alpha\beta t| < XY = N^{\delta+\gamma+\varepsilon-0.5}N^{0.5} = N^{\delta+\gamma+\varepsilon}. \tag{1}$$

We assume at this point of the proof that $\delta \geq 1/2$. We will later see that this assumption always holds and it is derived from the remaining solvability conditions of Theorem 4. Therefore, since $4\alpha\beta t < N^{\varepsilon+0.5}$, using our assumption $0.5 \leq \delta < \delta + \gamma$ we obtain that Equation (1) holds.

According to Theorem 4, we can find the solutions $x_0 = k$ and $y_0 = p+q$ to equation $xH(y) - 4\alpha\beta t \equiv 0 \bmod e$ if certain conditions are met.

Let consider the first case of Theorem 4. We have

$$0 \leq \frac{1}{2\delta} < \frac{1}{4} \Leftrightarrow 2 < \delta,$$

and

$$\frac{\delta + \gamma + \varepsilon - 0.5}{\delta} \leq \frac{3}{4} - \frac{0.5}{\delta} \Leftrightarrow \delta + \gamma + \varepsilon \leq \frac{3\delta}{4}$$
$$\Leftrightarrow \gamma \leq -\frac{\delta}{4} - \varepsilon.$$

Since we also want $\gamma > 0$, we obtain that in this case is not possible to solve the equation.

In the second case of Theorem 4 we have

$$\frac{1}{4} \leq \frac{1}{2\delta} \leq 1 \Leftrightarrow \frac{1}{2} \leq \delta \leq 2$$

and

$$\frac{\delta + \gamma + \varepsilon - 0.5}{\delta} \leq 1 - \frac{1}{\sqrt{2\delta}} \Leftrightarrow \delta + \gamma + \varepsilon - 0.5 \leq \delta - \sqrt{0.5\delta}$$
$$\Leftrightarrow \gamma \leq 0.5 - \varepsilon - \sqrt{0.5\delta}.$$

Since we also want $\gamma > 0$ we must have

$$0 < 0.5 - \varepsilon - \sqrt{0.5\delta} \Leftrightarrow \delta < \frac{(1-2\varepsilon)^2}{2}.$$

But we obtain a contradiction with

$$\frac{1}{2} \leq \delta < \frac{(1-2\varepsilon)^2}{2}.$$

Therefore, it is not possible to solve the equation. □

Remark 2. In a similar way, we can prove that we cannot factor N when $p < q < 2p$. Note that the only change in Theorem 5's proof is that we need to use the approximation $p - 1 \simeq \sqrt{N}$, instead of $q - 1 < \sqrt{N}$.

Theorem 6. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $e = N^{\delta}$, $2^{\lambda} = N^{\eta}$ and $d < N^{\gamma}$. We cannot recover the secret key r in polynomial time using the method presented in Theorem 4.*

Proof. By rewriting the key equation $ed - kr = 1$, we obtain the congruence $kr + 1 \equiv 0 \bmod e$. Consequently, we deduce the equation $xy + 1 \equiv 0 \bmod e$, which has k and r as solutions.

In order to be able to apply Theorem 4 we first need to bound k. Since $kr = ed - 1 < ed$ and $N^{\eta} < r$, we obtain that

$$k < \frac{ed}{r} < N^{\delta + \gamma - \eta}.$$

We also have that $r < 2N^{\eta}$. Therefore, we have that $k < X = e^{(\delta+\gamma-\eta)/\delta}$ and $r < Y \simeq e^{\eta/\delta}$.

According to Theorem 4, we can find the solutions $x_0 = k$ and $y_0 = r$ to equation $xy + 1 \equiv 0 \bmod e$ if certain conditions are met.

Let consider the first case of Theorem 4. We have

$$0 \leq \frac{\eta}{\delta} < \frac{1}{4} \Leftrightarrow 4\eta < \delta$$

and

$$\begin{aligned} \frac{\delta+\gamma-\eta}{\delta} \leq \frac{3}{4} - \frac{\eta}{\delta} &\Leftrightarrow \delta + \gamma \leq \frac{3\delta}{4} \\ &\Leftrightarrow \gamma \leq -\frac{1}{4}\delta. \end{aligned}$$

Since we also want $\gamma > 0$, we obtain that in this case is not possible to solve the equation.

In the second case of Theorem 4 we have

$$\frac{1}{4} \leq \frac{\eta}{\delta} \leq 1 \Leftrightarrow \eta \leq \delta \leq 4\eta$$

and

$$\begin{aligned} \frac{\delta+\gamma-\eta}{\delta} \leq 1 - \frac{\sqrt{\eta}}{\sqrt{\delta}} &\Leftrightarrow \delta + \gamma - \eta \leq \delta - \sqrt{\eta\delta} \\ &\Leftrightarrow \gamma \leq \eta - \sqrt{\eta\delta}. \end{aligned}$$

Since we also want $\gamma > 0$ we must have

$$0 \leq \eta - \sqrt{\eta\delta} \Leftrightarrow \delta \leq \eta.$$

But we obtain the following contradiction

$$\eta \leq \delta < \eta.$$

Therefore, it is not possible to solve the equation. □

4 Conclusions

In this paper, we presented two impossibility results for the Roman'kov scheme [17]. First, we showed that lattice attacks based on the results presented in [1,11] cannot be used to factor N. Then, in a similar manner, we showed that r also cannot be recovered. Since the bounds provided in Theorem 4 are optimal under reasonable assumptions, our results show that this class of lattice attacks do not seem work in the case of Roman'kov's scheme without substantial adaptations.

References

1. Abderrahmane Nitaj, N.N.H.A., Ariffin, M.R.B.K.: Cryptanalysis of a New Variant of the RSA Cryptosystem. In: AFRICACRYPT 2024. Springer (2024)
2. Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS **46**(2), 203–213 (1999)
3. Boneh, D., Durfee, G.: Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$. In: EUROCRYPT 1999. Lecture Notes in Computer Science, vol. 1592, pp. 1–11. Springer (1999)
4. Coppersmith, D.: Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In: EUROCRYPT 1996. Lecture Notes in Computer Science, vol. 1070, pp. 178–189. Springer (1996)
5. Coppersmith, D.: Finding a Small Root of a Univariate Modular Equation. In: EUROCRYPT 1996. Lecture Notes in Computer Science, vol. 1070, pp. 155–165. Springer (1996)
6. Coppersmith, D.: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology **10**(4), 233–260 (1997)
7. Cotan, P., Teşeleanu, G.: Small Private Key Attack Against a Family of RSA-Like Cryptosystems. In: NordSEC 2023. Lecture Notes in Computer Science, vol. 14324, pp. 57–72. Springer (2023)
8. Herrmann, M., May, A.: Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA. In: PKC 2010. Lecture Notes in Computer Science, vol. 6056, pp. 53–69. Springer (2010)
9. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: IMA 1997. Lecture Notes in Computer Science, vol. 1355, pp. 131–142. Springer (1997)
10. Jochemsz, E., May, A.: A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants. In: ASIACRYPT 2006. Lecture Notes in Computer Science, vol. 4284, pp. 267–282. Springer (2006)
11. Kunihiro, N.: On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree. In: ISC 2012. Lecture Notes in Computer Science, vol. 7483, pp. 55–69. Springer (2012)
12. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring Polynomials with Rational Coefficients. Mathematische Annalen **261**, 515–534 (1982)
13. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. thesis, University of Paderborn (2003)
14. May, A.: Using LLL-Reduction for Solving RSA and Factorization Problems. In: The LLL Algorithm: Survey and Applications, pp. 315–348. Information Security and Cryptography, Springer (2010)
15. Nitaj, A.: Another Generalization of Wiener's Attack on RSA. In: AFRICACRYPT 2008. Lecture Notes in Computer Science, vol. 5023, pp. 174–190. Springer (2008)
16. Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM **21**(2), 120–126 (1978)
17. Roman'kov, V.A.: New Probabilistic Public-key Encryption Based on the RSA Cryptosystem. Groups Complexity Cryptology **7**(2), 153–156 (2015)
18. Shi, G., Wang, G., Gu, D.: Further Cryptanalysis of a Type of RSA Variants. In: ISC 2022. Lecture Notes in Computer Science, vol. 13640, pp. 133–152. Springer (2022)
19. Wiener, M.J.: Cryptanalysis of Short RSA Secret Exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)